get complete pdf at learnexams.com

WGU C702 Forensics and Network Intrusion Exam (New 2023/ 2024 Update) Questions and Verified Answers| 100% Correct

QUESTION

Which application should a forensic investigator use to analyze information on a Mac OSX?

Answer:
Data Rescue 4

Which documentation should a forensic examiner prepare prior to a dynamic analysis?

Answer:
The full path and location of the file being investigated

QUESTION

What allows for a lawful search to be conducted without a warrant or probable cause?

learnexams

Answer:
Consent of person with authority

QUESTION

A forensic investigator is tasked with retrieving evidence where the primary server has been erased. The investigator needs to rely on network logs and backup tapes to base their conclusions on while testifying in court. Which information found in rules of evidence, Rule 1001, helps determine if this testimony is acceptable to the court?

Answer:
Definition of original evidence

QUESTION

When can a forensic investigator collect evidence without formal consent?

LEARNEXAMS.COM

get complete pdf at learnexams.com

Answer:
When properly worded banners are displayed on the computer screen

QUESTION
Who determines whether a forensic investigation should take place if a situation is undocumented in the standard operating procedures?

Answer:
Decision maker

QUESTION
Which situation leads to a civil investigation?

Answer:
Disputes between two parties that relate to a contract violation

learnexams

QUESTION
Which rule does a forensic investigator need to follow?

Answer:
Use well-known standard procedures

QUESTION
What is the focus of Locard's exchange principle?

Answer:
Anyone entering a crime scene takes something with them and leaves something behind.

QUESTION

LEARNEXAMS.COM

get complete pdf at learnexams.com

What is the focus of the enterprise theory of investigation (ETI)?

Answer:
Solving one crime can tie it back to a criminal organization's activities.

QUESTION
A forensic investigator is searching a Windows XP computer image for information about a deleted Word document. The investigator already viewed the sixth file that was deleted from the computer. Two additional files were deleted. What is the name of the last file the investigator opens?

Answer:
$R7.doc

QUESTION
What is a benefit of a web application firewall (WAF)?

Answer:
Acts as a reverse proxy to inspect all HTTP traffic

learnexams

QUESTION
How does a hacker bypass a web application firewall (WAF) with the toggle case technique?

Answer:
By randomly capitalizing some of the characters

QUESTION
During a recent scan of a network, a network administrator sent ICMP echo 8 packets to each IP address being used in the network. The ICMP echo 8 packets contained an invalid media access control (MAC) address. Logs showed that one device replied with ICMP echo 0 packets. What does the reply from the single device indicate?

LEARNEXAMS.COM